ALVEREAD
TECHNOLOGY FOCUS

Az OSINT lehetőségei a fake news és scam tartalmak vizsgálatában

A Bitcoin Loophole kampány OSINT-alapú vizsgálata

SECURITY TESTING LABORATORY
MAKING THE WORLD SAFER

Tartalom

Bevezető

A nyilvános forrású információgyűjtés (vagy nyílt forrású információgyűjtés) a neve és rövidítése (OSINT[1]) ellenére nem katonai vagy hírszerzés-specifikus tevékenység. Tény, hogy az OSINT módszereket előszeretettel használják a különféle szakszolgálatok és rendvédelmi szervek, azonban ezekkel a módszerekkel dolgoznak az újságírók, üzleti elemzők, és tulajdonképpen bárki, aki nyilvános forrásokból gyűjt össze információkat és használja fel azokat valamilyen cél érdekében.

Az OSINT „*a publikum (tehát minden egyén) számára nyilvánosan, legális eszközökkel megszerezhető, vagy korlátozott körben terjesztett, de nem minősített adatok szakmai szempontok alapján történő felkutatását, gyűjtését, szelektálását, elemzését-értékelését és felhasználását jelenti*[2]".

Az OSINT tehát egy információszolgáltató módszerként is értelmezhető, amely a felmerült kérdésekre igyekszik választ találni olyan eszközök alkalmazásával, amelyek bárki számára elérhetők, használatuk bárki számára megtanulható, és amelyek segítségével előállíthatók azok az információk, amelyekre a felhasználónak szüksége van a céljai eléréséhez.

Az OSINT módszerrel történő adatszerzés célja nagyon sokrétű lehet. A rendvédelem mellett említésre kerültek az újságírók, akik gyakran kutatnak és tárnak fel információkat tevékenységük során. Az üzleti elemzők az összegyűjtött információkból összefüggéseket állapítanak meg, amelyek alapján üzleti döntések születhetnek. De kiberbűnözők is alkalmazzák célpontjaik felderítésére, értékelésére és a támadások megtervezésére.

OSINT módszereket használhatnak a gyengeségeket, sebezhetőségeket felkutató, a kibervédelem oldalán dolgozó szakértők, vagy akár a különféle csalás elleni szervezetek. Alapozhatnak rájuk a hír- és tényellenőrző (*fact checker*) szolgáltatások, amelyek az álhírek leleplezésén és a források ellenőrzésén dolgoznak. OSINT módszereket és eszközöket használnak a hallgatók és diákok, amikor az elkészítendő szakdolgozathoz vagy egyéb feladataikhoz kutatásokat végeznek az interneten, Ugyanúgy, mint tanáraik, akik például plágiumkeresők használatával „szorosabb összefüggéseket" igyekeznek feltárni a nyilvános források és a beadott művek között.

A nyilvános forrású információgyűjtés láthatóan nem kötődik szakmához vagy hivatáshoz. Az ilyen keresés, kutatás és információgyűjtés bárki számára elérhető és megkönnyítheti céljai elérését.

Jelen tanulmány a Csányi Sándor, OTP Bank Nyrt. elnök-vezérigazgató nevével is visszaélő, csaló kriptovaluta kereskedési rendszer, a Bitcoin Loophole nemzetközi és hazai vonatkozású kampányait vizsgálja meg, OSINT módszerek és eszközök felhasználásával.

---

[1] *Open Source Intelligence, nyilvános forrású információgyűjtés*

[2] *Deák Veronika - Hadmérnök, XIII. Évfolyam 3. Szám – Lévay 2006, 6. alapján (http://www.hadmernok.hu/183_29_deak.pdf)*

A vizsgált kampány 2020. augusztus 10-én vált ismertté, amikor több hazai médium is felhívta a figyelmet, hogy a 24.hu internetes újság arculatával megjelenő oldal Csányi Sándor nevével visszaélve próbálja meg kicsalni az extra nyereségre vágyók pénzét.

A tanulmány célja, hogy nyilvános forrású információgyűjtés (OSINT) segítségével megállapítsa a kampány esetleges előzményeit és nemzetközi kapcsolatait, működési metódusait, terjedési sémáit, valamint összefüggést találjon az álhírek (fake news) és a különféle, kriptovalutákat és kereskedési platformokat felhasználó internetes csalások és átverések (scam) között.

A Bitcoin Loophole

A Bitcoin Loophole egy jól ismert, a Bitcoin kereskedelmére épülő átverés/csalás (*scam*), amely 2018-ban vált ismertebbé, és amelyre már több fraud-monitoring és csalás elleni szervezet is felhívta a figyelmet. A Bitcloin Loophole magát irreálisan magas hozamokat ígérő, mesterséges intelligenciával támogatott kereskedési rendszernek állítja be, amely a valóságban csak arra szolgál, hogy a befektető pénzét kicsalja.

Nemzetközi szinten több kormányzati intézmény is figyelmeztet a csalásra, például a brit pénzügyi felügyelet (FCA - Financial Conduct Authority) 2018. júniusában tette közzé a Bitcoin Loophole-lal kapcsolatos jelzését[3], a szingapúri pénzügyi felügyelet (MAS - Monetary Authority of Singapore) pedig 2019. júliusában jelentetett meg egy értesítést[4], miszerint a szingapúri felügyelet elnökének (és egyben korábbi szingapúri miniszterelnöknek) nevét használták fel a szolgáltatás reklámozására[5].

A Magyar Nemzeti Bank oldalán elérhető olyan kereső[6], amely a társfelügyeletektől érkező figyelmeztetéseket tartalmazza. A keresőben a Bitcoin Loophole neve még nem szerepel, azonban megtalálható több olyan szolgáltatással kapcsolatos nemzetközi figyelmeztetés, amelyek közvetlenül is kapcsolatba hozhatók a Bitcoin Loophole-lal (például *Bitcoin Revolution, Bitcoin Era, Bitcoin Evolution*).

Társaság neve	Küldő társhatóság megnevezése
BITCOIN REVOLUTION	Comisión Nacional del Mercado de Valores (CNMV) - spanyol felügyelet
Bitcoin Revolution	Malta Financial Services Authority - máltai felügyelet
Bitcoin-Evolution / Bitcoin-Revolution	Financial Services and Markets Authority- belga felügyelet

MNB kereső társhatóságok által küldött figyelmeztetésekre

[3] *https://www.fca.org.uk/news/warnings/bitcoin-loophole-bitcoin-news-trader*

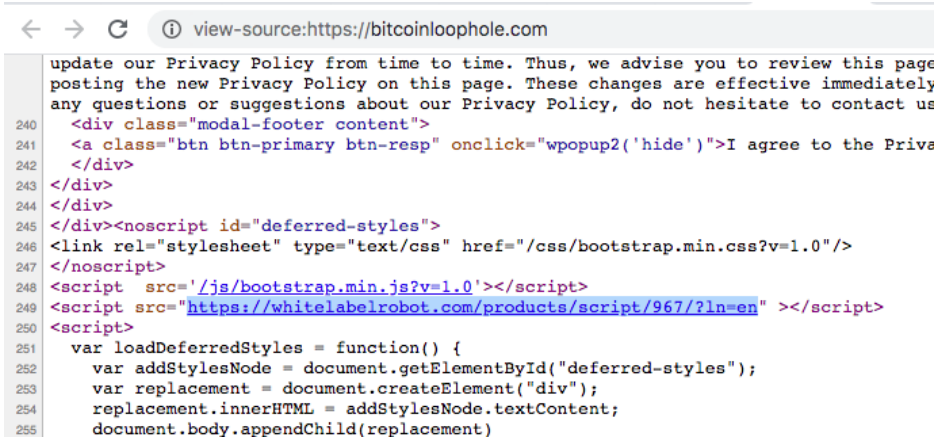
[4] *https://www.mas.gov.sg/news/media-releases/2019/warning-on-fraudulent-website-soliciting-bitcoin-investments*

[5] *https://www.mas.gov.sg/-/media/Annex---Screenshot-of-the-Website.pdf*

6 http://alk.mnb.hu/figyelemsearchf/listall illetve https://www.mnb.hu/kulfoldi-figyelmeztetesek

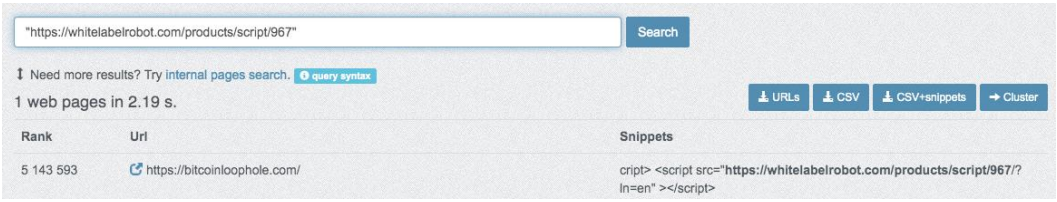
A Bitcoin Loophole internetes háttere

A *bitcoinloophole.com* oldal nem tartalmaz Google hirdetői azonosítókat (AdSense vagy Analytics ID), így azokon keresztül nem hozható kapcsolatba más weboldallal, tartalmaz viszont egy ajánló (*affiliate*) rendszerhez tartozó scriptet (*whitelabelrobot.com*).



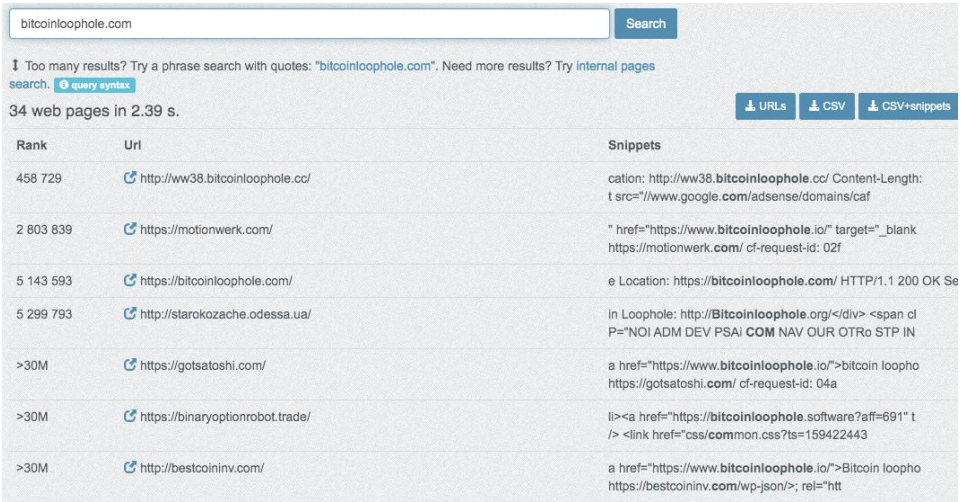
A Whitelabelrobot affiliate rendszer használatához szükséges script

A *PublicWWW*, vagy más kódrészletkereső eszköz segítségével megállapítható, hogy a *bitcoinloophole.com* oldalon kívül más oldal nem tölti be ezt az affiliate scriptet és nem használja ezt az azonosítót. A kódkeresők azt vizsgálják, hogy a keresett kódrészlet milyen más weboldalakban szerepel. Jelen esetben ez a vizsgálat nem hozott eredményt.



Az affiliate rendszeren keresztül nem lehet másik oldallal összekapcsolódni

A kódrészletkereső segítségével a Bitcoin Loophole weboldal összekapcsolható más olyan weboldalakkal, amelyek vagy hivatkoznak a *bitcoinloophole.com* címre, vagy ahhoz nagyon hasonló címekre.



Közvetett kapcsolatok a Bitcoin Loophole szolgáltatással

A Bitcoin Loophole szolgáltatással közvetetten kapcsolatba hozható tartalmak	
http://ww38.bitcoinloophole.cc/	http://starokozache.odessa.ua/
https://gotsatoshi.com/	http://bestcoininv.com/
http://bitcoinloophole.site/	https://bitcoin-loophole.net/
https://loopholebit.com/	https://bitcoinloophole.software/
http://bitcoinloophole.org/	http://bitcoinloopholeappwh.com/
http://bitcoinloopholeappsoft.com/	https://lrmcoin.com/
https://www.bitcoinloophole.app/	http://bitcoin-loophole-appsoft.com/
https://bitcoin-loophole.org/	https://en.bitcoinloophole-app.com/
https://leloophole.com/	http://bitcoinloophole.ltd/
http://thebitcoinloophole.club/	http://btcloopholeweb.com/
http://bitcoinloophole2web.com/	https://bitcoinloophole.global/
https://bitcoinloophole.space/	http://bitcoinloophole.xyz/
https://bitcoin-loophole.com	https://bitcoinloopholes.com
https://bitcoinsloophole.com	

IP és DNS historikus keresők (például *DNSlytics*) segítségével megállapítható, hogy a *bitcoinloophole.com* domainhez legalább 2014. októbere óta tartozik valamilyen IP cím, azaz a *bitcoinloophole.com* domaint már 2014-ben beregisztrálták.

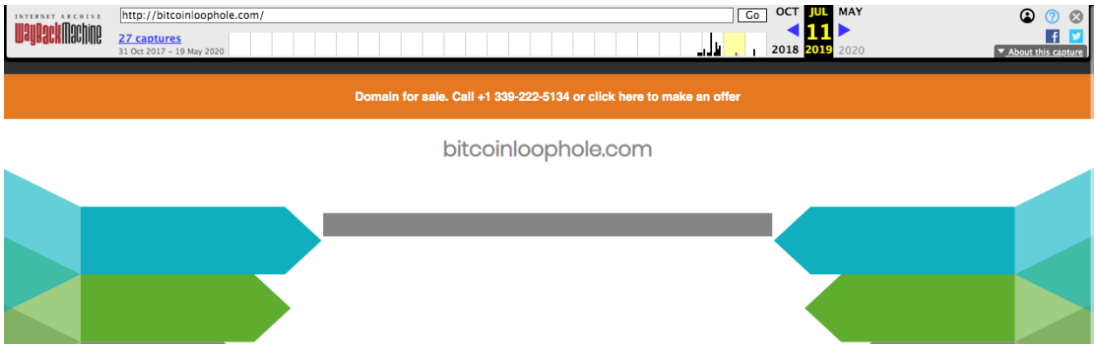
#	IPv4 address	Last seen	Tools
1	94.23.247.193	2020-08-30	IP History Whois+
2	185.53.178.8	2019-07-16	IP History Whois+
3	185.53.179.6	2019-06-13	IP History Whois+
4	185.53.178.7	2019-05-27	IP History Whois+
5	185.53.178.8	2019-01-08	IP History Whois+
6	54.72.9.51	2018-12-13	IP History Whois+
7	198.54.117.200	2018-10-25	IP History Whois+
8	198.57.246.6	2018-09-09	IP History Whois+
9	8.5.1.40	2014-12-08	IP History Whois+
10	66.147.244.78	2014-10-12	IP History Whois+

IP history lekérdezése, az IP legalább 2014 októbere óta üzemel

A *Wayback Machine*[7] internetes archívum szerint azonban a *bitcoinloophole.com* oldalon csak 2017-től érhető el tartalom, a korábbi időszakról nincs adat az archívumban. A Wayback Machine 2017. október 31-én készített először mentést az oldalról[8], az első snapshoton a „*This offer is not*

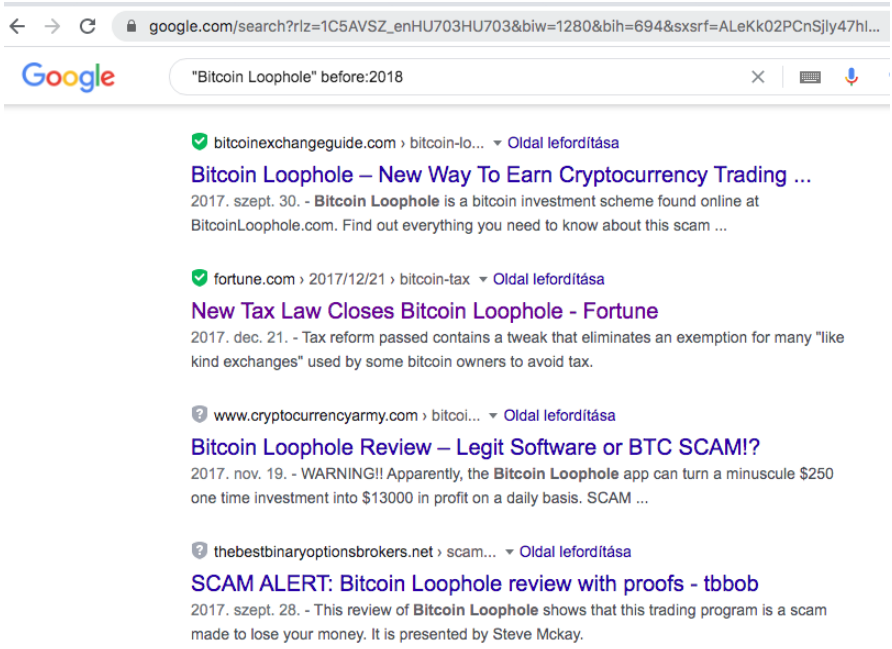
[7] *https://web.archive.org/web/*/bitcoinloophole.com*
[8] *https://web.archive.org/web/20171031062214/http://www.bitcoinloophole.com/*

available in your location" üzenet található. A Wayback Machine 2019. július 11-én készült mentése[9] alapján a domain eladó státuszba került.



Eladó a bitcoinloophole.com domain

A Wayback Machine 2020. május 19-én készített mentése az első, ahol a jelenlegi formájában látható a weboldal. A ScamBroker szerint a Bitcoin Loophole már 2018. januárjában kínálta a szolgáltatását[10], míg a Fortune magazin cikke alapján már 2017-ben megkezdte a tevékenységet[11].



Google keresés 2018-at megelőző Bitcon Loophole tartalmakra

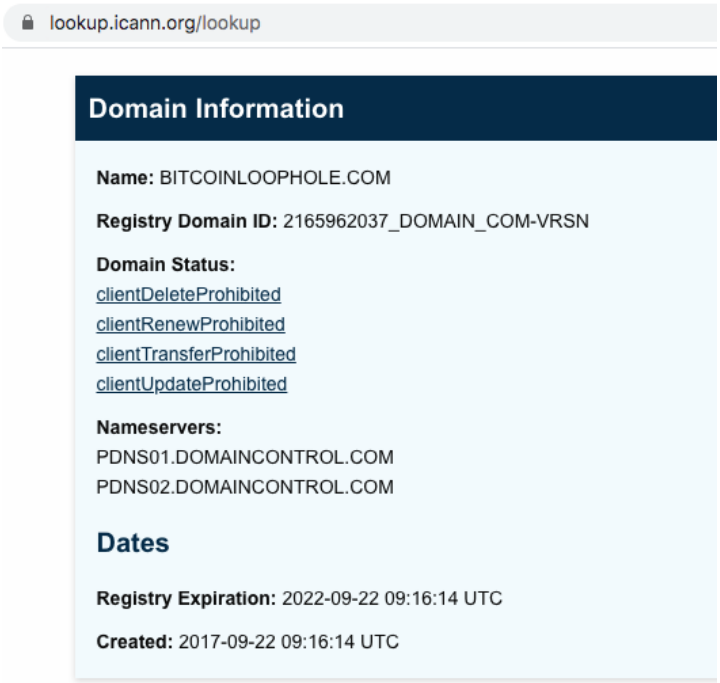
Az eltérő időpontokra (és Wayback Machine archívumban nem szereplő időszakokra) magyarázat lehet, hogy bár a domaint 2014-ben jegyezték be először, az több alkalommal is megszüntetésre, illetve újra regisztrációra kerülhetett. Ezt a feltevést erősíti meg a 2019. júliusi értékesítésre vonatkozó Wayback Machine mentés, valamint egy 2015-ös, lejáró domainek listájában szereplő bejegyzés.

---

[9] *https://web.archive.org/web/20190711160620/http://bitcoinloophole.com/*
[10] *https://scambroker.com/bitcoin-loophole/*
[11] *https://fortune.com/2017/12/21/bitcoin-tax/*

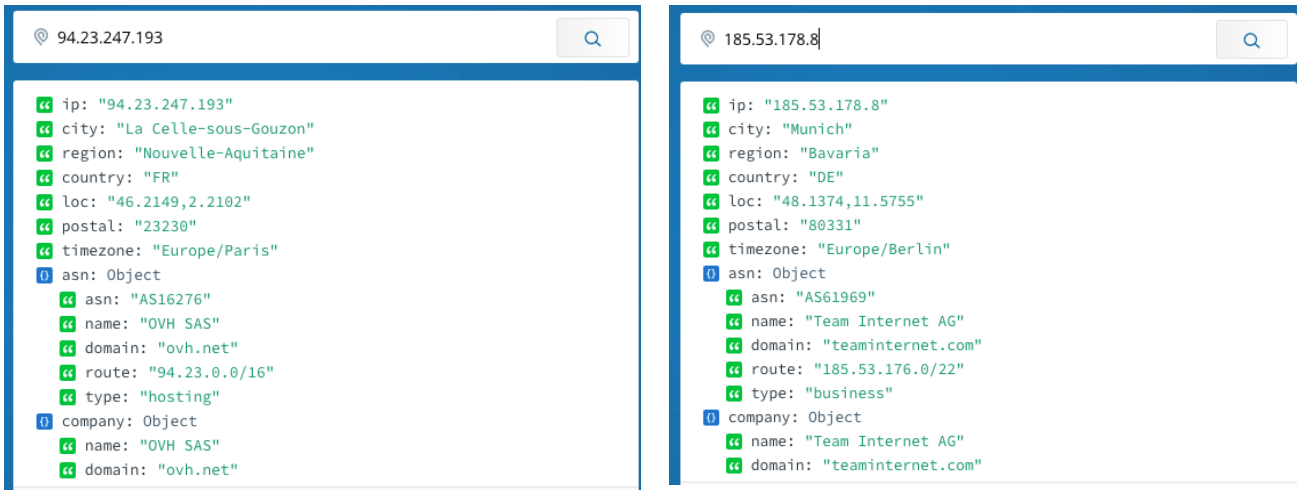
A domain 2015-ben is meghírdetésre került, mint megújításra nem került domain

A jelenleg ismert Bitcoin Loophole oldal és tartalom (azaz maga a szolgáltatás) keletkezése feltehetőleg 2017-re datálható. Ezt erősíti meg egyrészt a Fortune magazin cikke, másrészt pedig az internetes domain delegálási szabályokat meghatározó *Internet Corporation for Assigned Names and Numbers* (ICANN) szervezet keresőjében található információ, amely a domain legutolsó ismert regisztrációs dátumára vonatkozik.



A bitcoinloophole.com domain utolsó regisztrációs dátuma 2017. szeptember 22.

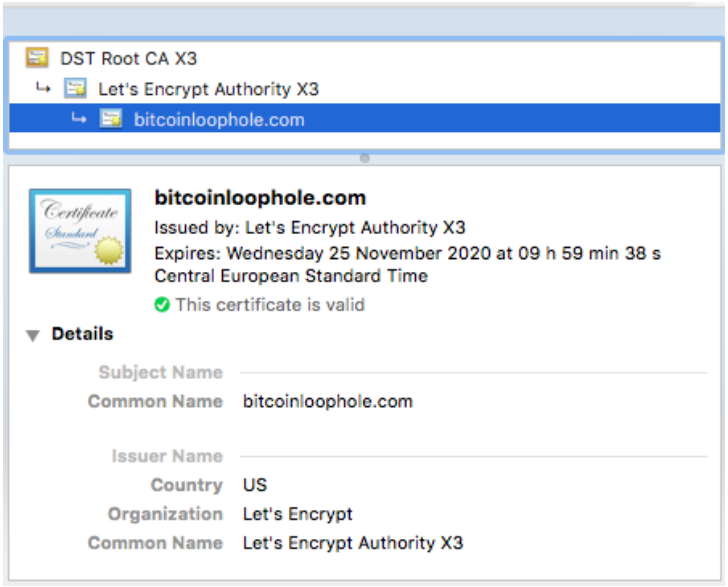
A jelenlegi IP cím (94.23.247.193) és geolokációs kereső (például az *IPInfo*) alapján az oldal egy francia tárhelyszolgáltatónál működik, de 2014-ig visszamenőleg legalább 10 IP címen volt elérhető a domain valamilyen formában (például parkolt, nem használt domain).



Jelenleg egy francia szolgáltatónál működik, de 2019-ben egy müncheni szolgáltatónál üzemelt

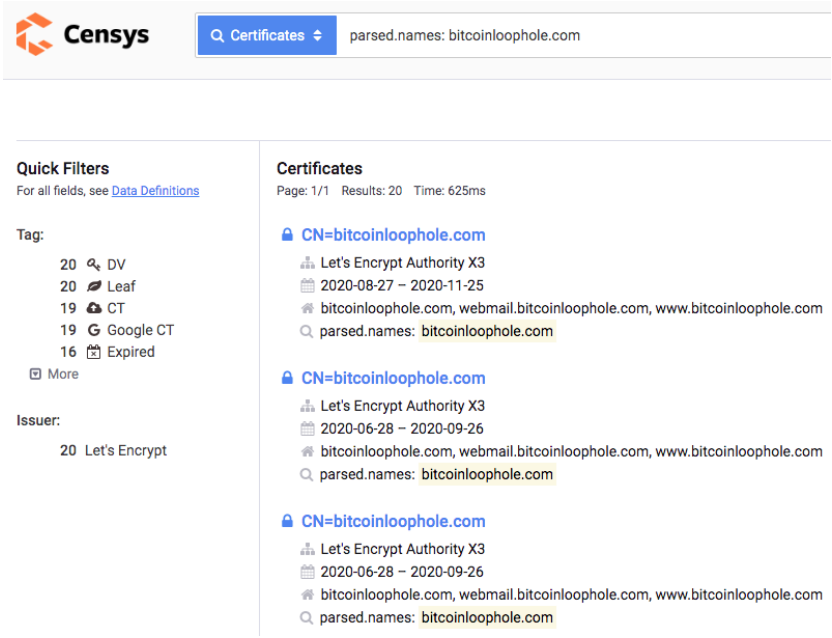
A Bitcoin Loophole weboldala saját kibocsátású Lets Encrypt HTTPS/SSL tanúsítványt használ, amely mindenképpen szokatlan egy „pénzügyi szolgáltató" vagy „*trading platform*" esetében.

A Let's Encrypt egy ingyenes, automatizált, nyílt forrású tanúsítvány hitelesítő az *Internet Security Research Group* (ISRG) jóvoltából, amely lehetővé teszi, hogy költség nélkül bárki képes legyen megbízhatónak *vélhető* tanúsítványt kiállítani a saját weboldalához. A pénzügyi szolgáltatók azonban megbízható hitelesítő szervezetektől vásárolják a tanúsítványaikat, így azok minden esetben hitelesnek és megbízhatónak tekinthetők.



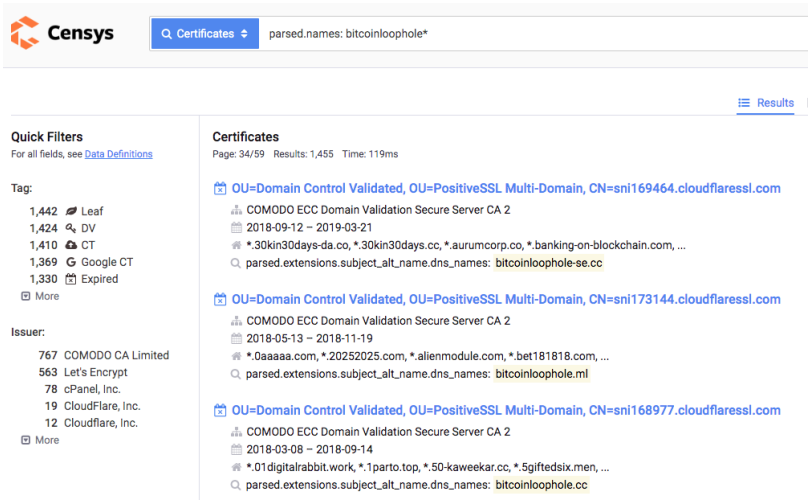
A bitcoinloophole.com tanúsítványa nem tartalmaz a szervezetre vonatkozó információkat

A *Censys* eszközkeresőt használva megállapítható, hogy csak a *mail.bitcoinloop.com*, *webmail.bitcoinloop.com* és *www.bitcoinloophole.com* címekre lettek tanúsítványok kiállítva.



bitcoinloophole.com címre kiállított tanúsítványok

A Censys eszközkeresőben lehetőség van a tanúsítványadatok és paraméterek között keresni. Segítségével megállapítást nyert, hogy összesen 1455 olyan tanúsítvány található, amelynek szerver vagy domain címében szerepel a „*bitcoinloophole*" kifejezés.



1455 találat "bitcoinloophole" kifejezést tartalmazó tanúsítványokra

A korábbi módszerekkel, például a kódrészlet-kereséssel is lehet közvetett kapcsolatot találni az eredeti oldal (valamint a Bitcoin Loophole „szolgáltatás") és egyéb weboldalak között. A tanúsítvány vizsgálatával azonban jobban kirajzolódik, hogy milyen méretű a Bitcoin Loophole köré szerveződő hálózat: legalább 1455 olyan címből áll, amely valamilyen módon részt vesz a Bitcoin Loophole kampányok kiszolgálásában.

Azt nem lehet egyértelműen megállapítani, hogy az így kapcsolatba hozható oldalak és tartalmak közvetlenül az eredeti oldal irányítása alá tartoznak, viszont mindenképpen szereplői a Bitcoin Loophole köré szerveződő csalásnak.

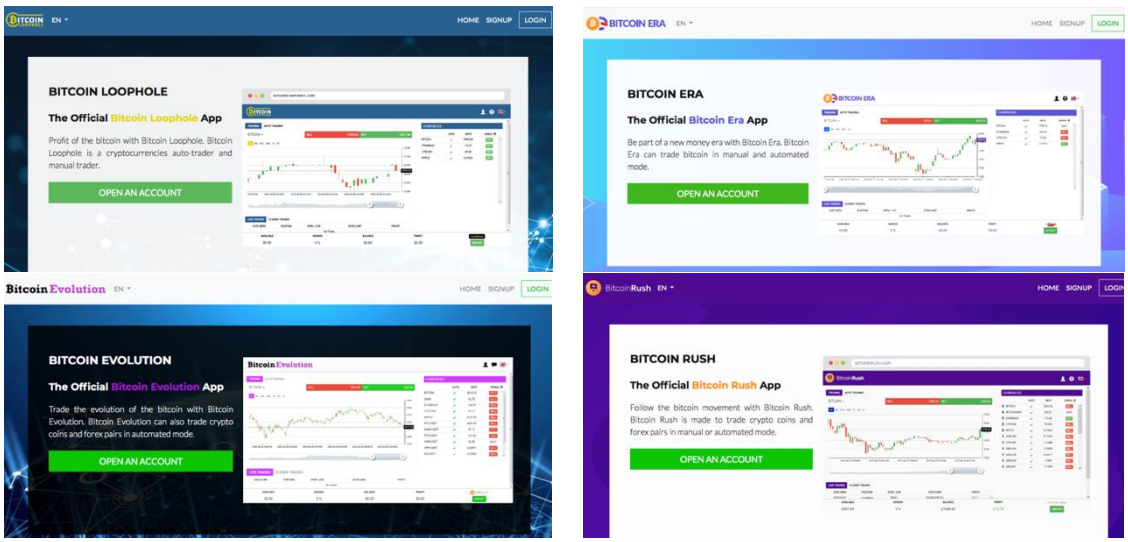
Vannak azonban olyan weboldalak és „szolgáltatások", amelyek közvetlenül is kapcsolatba hozhatók a Bitcoin Loophole oldallal. A *bitcoinloophole.com* IP címéhez társított domain címeket

ellenőrizve 25 további weboldal található, amelyeket nem csak ugyanez a szerver szolgál ki, de közvetlenül kapcsolódnak a Bitcoin Loophole köré szerveződött hálózathoz. A reverse IP keresésekkel feltárható, hogy egy adott IP címhez milyen domain nevek vannak társítva.

Reverse IP keresés, az IP címhez társított domainek (*DNSLytics*)

A bitcoinloophole.com oldallal közvetlenül kapcsolatba hozható tartalmak		
auroratrader.software	bitcoin-trader.biz	bitcoincode.global
bitcoinera.com	**bitcoinevolution.com**	bitcoinfuture.com
bitcoinloophole.com	bitcoinloophole.global	**bitcoinrevolution.software**
bitcoinrush.com	cannabistrader.software	crypto-advantage.com
cryptosoft.global	fintechltd.software	fxtrading.software
libratrader.com	ripplecode.software	roulettestrategy.software
teslerapp.software	thebitcoincode.software	thebitcoinmethod.software
thebitcoinrush.com	theethereumcode.software	weedtrader.software
win500aday.com	winroulettebot.com	

A 94.23.247.193 IP címhez társítható domainek között megtalálhatók a Bitcoin Era, Bitcoin Evolution és Bitcoin Revolution, a Bitcoin Loophole-hoz hasonló csalók, amelyeknek szintén van hazai kapcsolata és előzménye, és amelyekre az MNB nemzetközi társhatóságai is figyelmeztetést adtak ki.



Az IP cím több hasonló tartalmat is kiszolgál

A szerveren működő oldalak ugyanarra a csalási sémára (és hasonló „kereskedési alkalmazásra") épülő tartalmak. Megállapítható tehát, hogy a Bitcoin Loophole egy jól működő és több lábon álló crypto-fraud (vagy crypto-scam) csoporthoz tartozó szolgáltatás, amely évek óta többféle név és szolgáltatási cím alatt működik.

A Bitcoin Loophole hazai megjelenésének vizsgálata

Nyilvánossága és megjelenése

A Csányi Sándor nevét felhasználó Bitcoin Loophole scam hazai megjelenésével kapcsolatban a legkorábbi információ 2020. augusztus 7-ről származik: egy Index.hu fórumban bukkant fel a *https://newsline.to/sandor-csanyi-reveals-wealth-secret-hu/* link.

"Csányi S gazdaggá tesz?" topik, topiknyitó poszt

A topikban többen is jelezték, hogy a tartalom nem érhető el. Ennek feltételezhető oka, hogy a scam landing oldal csak a megfelelő ajánló (*referer*) fejlécelem esetén töltődik be. Amennyiben a referer hiányzik (azaz nem a reklámot megjelenítő oldalról érkezik a látogató, hanem a címet közvetlenül hívja meg), egy 404 hibaoldal jelenik meg. A későbbiekben bemutatásra kerül ez a metódus.

A Bitcoin Loophole szélesebb körben 2020. augusztus 10-én vált ismertebbé, amikor több hazai befektetési és híroldalon megjelent, hogy Csányi Sándor nevével, csalási szándékkal reklámoznak Bitcoin-alapú kereskedési és befektetési lehetőségeket.

Az „*Az én pénzem*[12]" pénzügyi tanácsadó oldalon megjelenő képernyőfotón kivehető, hogy ugyanaz a *https://newsline.to/sandor-csanyi-reveals-wealth-secret-hu/* link szerepel a böngészősávban, mint amelyre a fórumtopik három nappal korábban hivatkozott.

[12] *https://azenpenzem.hu/cikkek/az-otp-vezer-nevevel-elnek-vissza-a-csalok/7006/*

"Az én pénzem" pénzügyi tanácsadó oldal (2020 augusztus 10)

A *https://newsline.to/sandor-csanyi-reveals-wealth-secret-hu/* oldal a megfelelő ajánló (referer) fejlécelem nélkül nem érhető el, azonban ugyanez a tartalom jelenleg is elérhető a https://newsline.to/hu-sandor-csanyi-loophole/ oldalon, a *https://superscienceway.com/hu/* linken (referer oldal) keresztül.

A scam első változata, "*áhítatlankodnak*" verzió

A különféle híroldalak és szakportálok is kiemelték, hogy a scam a 24.hu internetes hírportál arculatát felhasználva „*szinte tökéletes magyarsággal, profi módon*[13]" lett kidolgozva.

A tartalomtól (hiteltelen és hihetetlen nyereségű ajánlat) eltekintve a nyelvezetből feltételezhető, hogy nem egyszerűen csak fordító programmal készült, bár a bevezetőben szereplő

[13] *https://www.bitcoinbazis.hu/csanyi-sandor-neveben-probalnak-meg-kriptopenzeket-kicsalni-gyanutlan-internetezoktol/*

„áhítatlankodnak" kifejezés, valamint néhány megfogalmazás, például „*A történelemben még soha nem volt ilyen csodálatos lehetőségünk, amit a hétköznapi emberek könnyen kihasználhatnak, hogy óriási vagyont halmozzanak, ilyen rövid idő alatt.*" árulkodhatnak arról, hogy megtévesztő és csalási szándékú oldalt lát az olvasó.

Előzmények, korábbi kampányok, változatok

A Csányi Sándor nevét felhasználó Bitcoin Loophole álhírnek és scam-nek létezik korábbi változata is, amely nem a newsline.to oldalon jelent meg, hanem az olkt.net oldalon.

„Áhítatlankodtalanított" verzió, OLKT.NET

Az *olkt.net* az „*Orbán Lapjáról Kitiltottak Társasága*" fórumcsoportból alakult, és az Urbanlegends által összeállított „*Megtévesztő magyar híroldalak listája 2020*[14]" gyűjtemény politikailag elfogult kategóriájában szerepel. A Pesti Srácok oldal a „*Számok – a baloldali álhírek ellenszere*[15]" csoportra hivatkozva megnevezte[16] az OLKT mögött álló személyeket és egy 24 oldalból álló kormányellenes álhírgyártó hálózattal hozta összefüggésbe őket.

A OLKT verzió és a híroldalak által felkapott *newsline.to* verzió között nyelvezeti és szövegezési szempontból jelentős eltérés nincs, a legfőbb különbség az „*áhítatlankodnak*" kifejezés hiánya a címsorban, tehát az oldalak feltételezhetően ugyanannak a kampánynak a részei. Ezt erősíti meg, hogy az OLKT verzióban a linkek a *https://newsline.to/sandor-csanyi-reveals-wealth-*

[14] *https://www.urbanlegends.hu/2020/01/megteveszto-magyar-hiroldalak-listaja-2020/*
[15] *https://www.facebook.com/szamokadatok/posts/164440465033095*
[16] *https://pestisracok.hu/megmutatjuk-kik-allnak-ket-nagy-alhirgyar-oldal-mogott-amelyek-oriasi-halozatot-mukodtetnek/*

secret-hu címre mutatnak. (Ez az URL nem elérhető, azonban ugyanerről a szerverről jelenleg is elérhető a megfelelő ajánlóval a *https://newsline.to/hu-sandor-csanyi-loophole cím*.

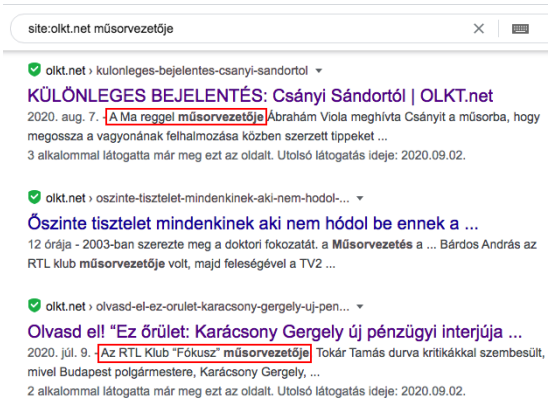
Az OLKT oldalon, illetve *https://newsline.to/hu-sandor-csanyi-loophole* oldalon megjelenő tartalom közötti kapcsolat a felhasznált képi elemek vizsgálatával is megerősíthető. Bár az OLKT tartalom esetében csak egyetlen kép került kiemelésre, a *newsline.to* pedig sokkal több képet tartalmaz, közös pontként meghatározható a Csányi Sándort ábrázoló fotó.

https://newsline.to/hu-sandor-csanyi-loophole/images/andrewf1.jpg

https://olkt.net/wp-content/uploads/2020/08/andrewf3-750x430.jpg

A képek csak hasonlóak, azonban mindkét fájlnévben szerepel az „*andrewf*" karaktersor, amely hasonlóság nem véletlenszerű (feltehetőleg egy, az Andrew Forrest nevével visszaélő kampány sablonjának másolata).

A Csányi Sándor nevét felhasználó OLKT tartalom a „hitelességet" erősítve a Ma reggel műsorvezetőjére, Ábrahám Violára hivatkozik. Mivel a hasonló nemzetközi kampányokban gyakran hivatkoznak televíziós műsorvezetőkre, ezért a Google-ban az OLKT oldalát megadva és a „*műsorvezetője*" kulcsszóval kiegészítve egy 2020. július 9-i tartalom[17] is megjelenik, amely Karácsony Gergely nevét használja fel a Bitcoin Era scam reklámozására.



Karácsony Gergely nevével visszaélő scam az OLKT oldalon

A Karácsony Gergely nevét felhasználó Bitcoin Era scam nyelvezetében sokkal primitívebb, mint a Csányi Sándor nevével operáló Bitcoin Loophole, ezért feltehetőleg egy korai változatról van

[17] *https://olkt.net/olvasd-el-ez-orulet-karacsony-gergely-uj-penzugyi-interjuja-gazdagga-teheti-a-magyarokat/*

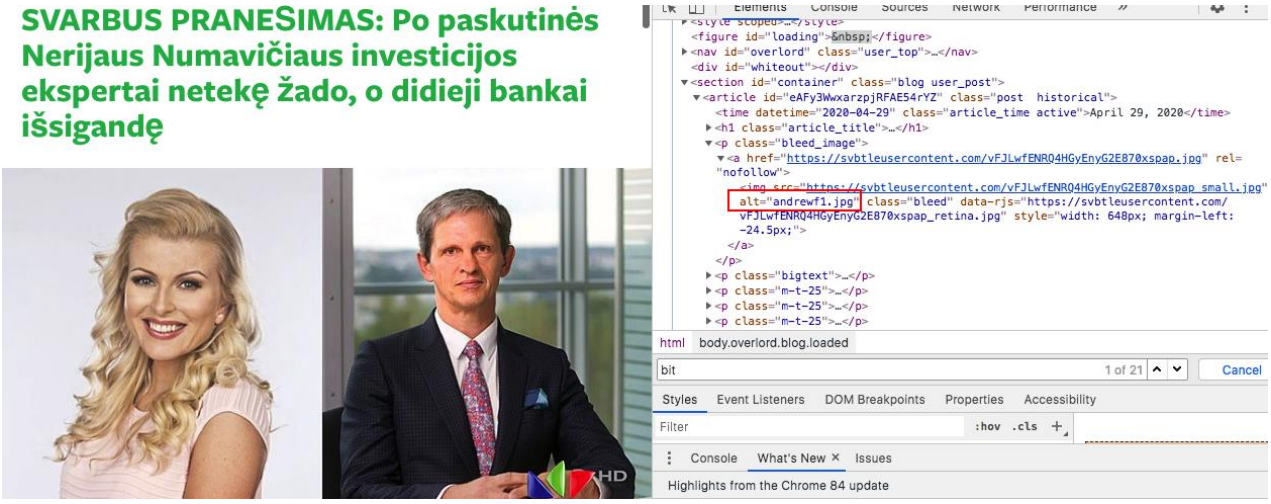
szó, amely esetében egyértelműnek tűnik, hogy egy külföldi személy nyelvi fordítóval készítette a tartalmat.

Karácsony Gergely személye már korábban is célkeresztbe került egy hasonló kripto-fraud kampányban. 2020. február 5.-én a FintechRadar jelentetett meg egy figyelmeztetést[18] azzal kapcsolatban, hogy Karácsony Gergely nevére hivatkozva internetes csalók reklámoznak Bitcoin Revolution csalásra épülő szolgáltatást.

A cikkben szereplő, a csaló oldalról kiemelt idézetek megtalálhatók a jelenleg is elérhető OLKT.NET oldalon[19], azonban az oldal nem a Bitcoin Revolution, hanem a Bitcoin Era reklámját tartalmazza.

Képi egyezések vizsgálata

A Bitcoin Loophole, illetve a hasonló nemzetközi kampányok további vizsgálatával található olyan tartalom, ahol a képek elnevezései egyeznek, vagy a képek ALT paraméterében benne maradt az „*andrewf*" karaktersor.



A litván milliárdos és befektető Nerijus Numavičius nevével visszaélő Bitcoin Revolution scam[20]

A képi elemek és a nevek hasonlóságát vizsgálva megállapítható, hogy a Bitcoin Loophole, illetve a sémára épülő hasonló „szolgáltatások" esetében a landing oldalak keretszerkezete és a felhasznált képi tartalmak ismétlődnek, ugyanazok a fotók kerülnek felhasználásra az egyes oldalakon, legfeljebb a vonatkozó szöveges tartalmakat aktualizálják és frissítik.

[18] *https://fintechradar.hu/befektetes/0206/uj-a-magyarokat-celzo-kriptos-atveres-bukkant-fel/*
[19] *https://olkt.net/olvasd-el-ez-orulet-karacsony-gergely-uj-penzugyi-interjuja-gazdagga-teheti-a-magyarokat/*
[20] *https://aproffnews.svbtle.com/svarbus-pranesimas-po-paskutines-nerijaus-numaviciaus-investicijos-ekspertai-neteke-zado-o-didieji-bankai-issigande*

A múlt héten szerepelt a Ma reggel műsorában, és bejelentett egy új **"vagyonosodási kiskaput"**, amely segítségével 3-4 hónapon **belül bárki milliomossá válhat**. Csányi sürgetett minden magyart, hogy éljen ezzel a csodálatos lehetőséggel, mielőtt a nagy bankok örökre megszüntetnék azt.

És eléggé biztosnak tűnik, mert az interjú után néhány perccel az OTP Bank felszólította a TV csatornát, hogy állítsák le Csányi interjújának sugárzását - de már túl késő volt.

Ez történt pontosan:

A Ma reggel műsorvezetője **Ábrahám Viola** meghívta **Csányit** a műsorba, hogy megossza a vagyonának felhalmozása közben szerzett tippeket és a magyar vállalkozó és emberbarát szinte bombát robbantott:

PROFIT: 4,824,411 HUF

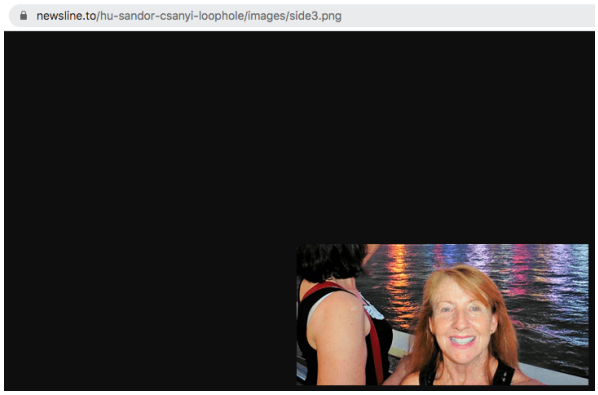
"Még nekem is rohadt egyszerű használni! Soha nem kereskedtem, de hetente 3000 dollárt keresek, és imádom ezt az életet!"

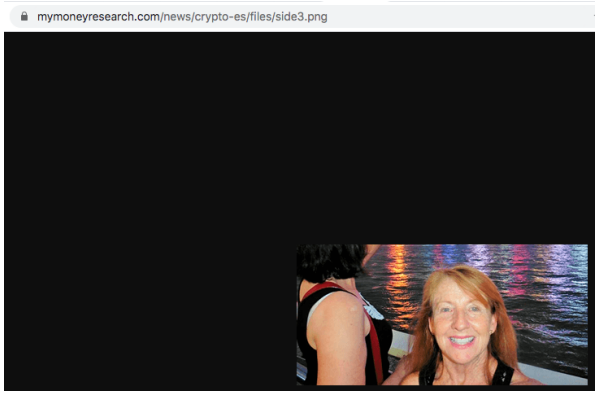
Honvéd Júlia
Debrecen

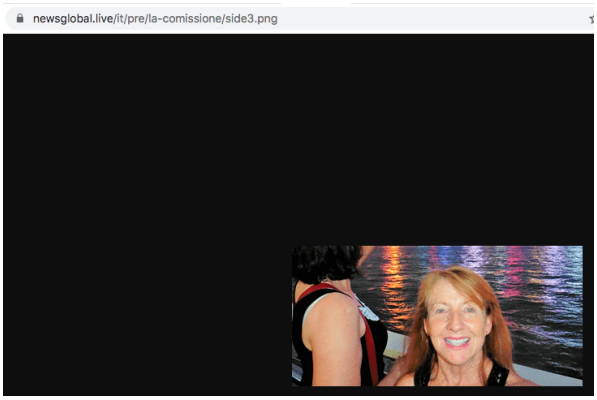
"Honvéd Júlia" a rendszer boldog felhasználója

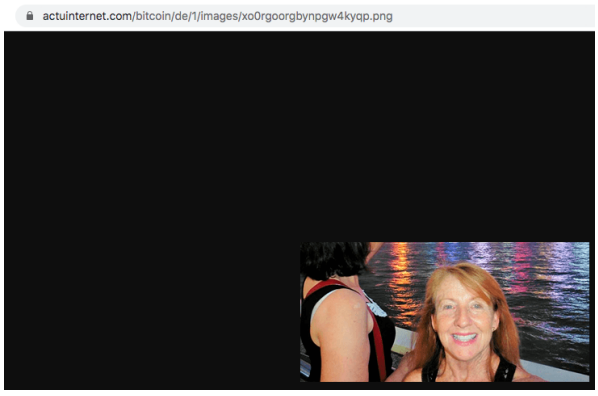
Reverse képkeresés, "Honvéd Júlia" több mint 200 hasonló tartalomban található meg

A képi tartalmak esetében a fájlnevek többnyire ugyanazok maradnak, illetve a fentebbi példában látható, hogy ha a fájlnév esetleg megváltoztatásra került, a kép ALT paraméterében benne maradhattak az eredeti fájlnév hivatkozások.

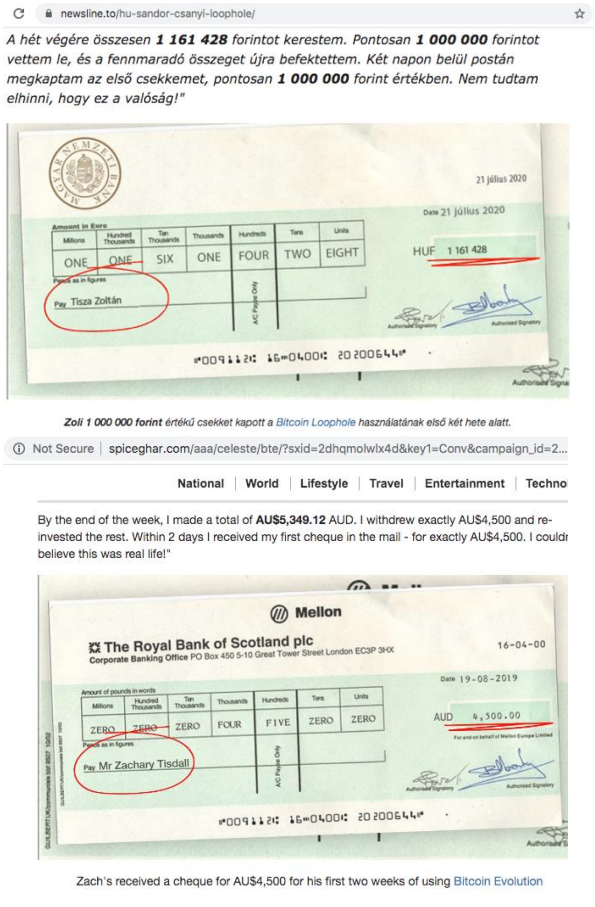








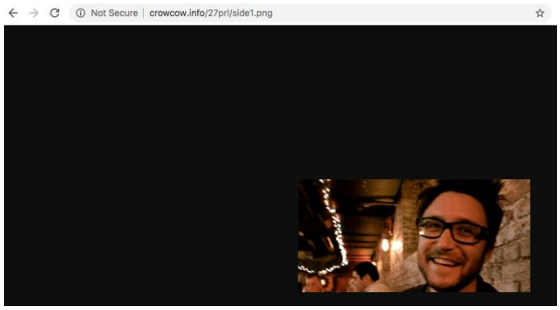
"Honvéd Júlia" a Bitcoin Loophole, Bitcoin Era, Bitcoin System tartalmakban

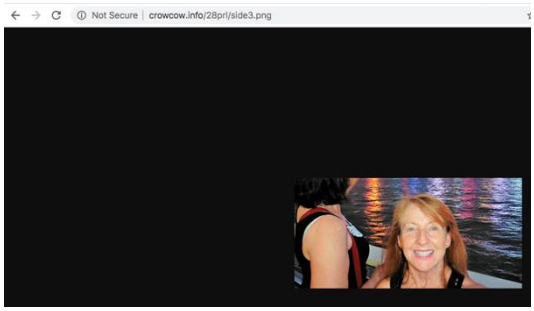


"Tisza Zoltán" és "Zachary Tisdall" Bitcoin Loophole és Bitcoin Evolution tartalmakban

A képi egyezőségek feltételezik, hogy a kampányok aktorai valamilyen sablonrendszert használnak az egyes landing oldalak és az álhírek elkészítéséhez.

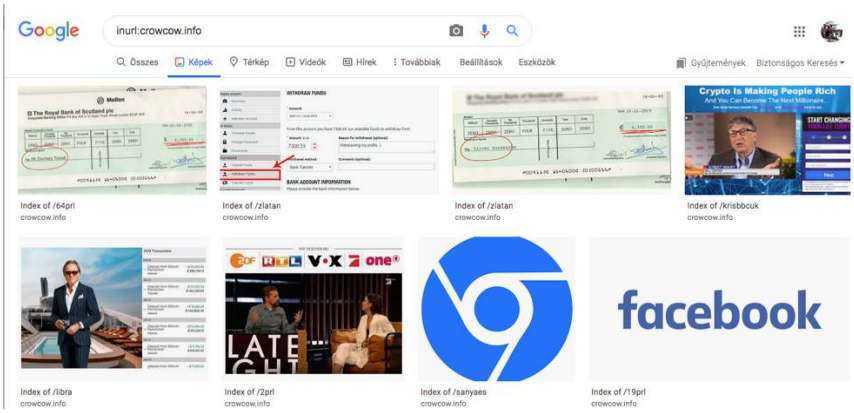
A képek nevére történő további keresésekkel hozzáférhető volt egy olyan mappastruktúra, amely hasonló kampányok landing oldalainak fájljait és sablonjait tartalmazta.

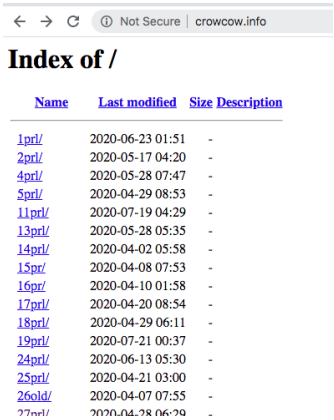




A crowcow.info oldalról származó side1.jpg és side3.jpg

A *crowcow.info* oldalra keresve a Google kereső olyan mappákat listázott, amelyekben láthatóan a scam kampányok állományai voltak megtalálhatók.



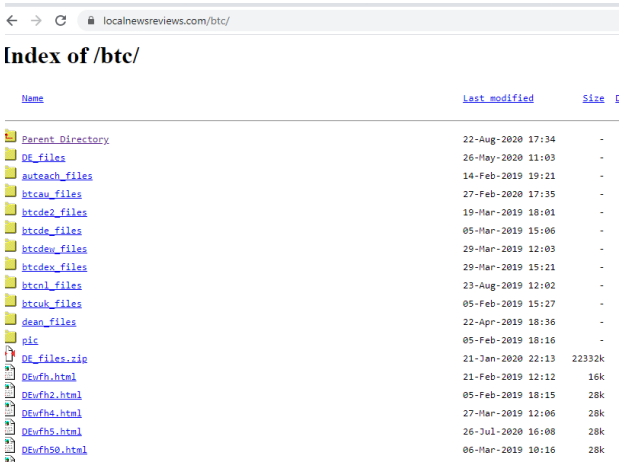


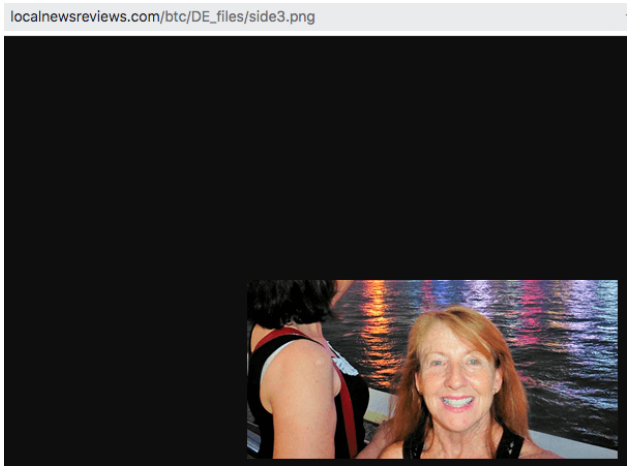
A crowcow.info oldalon található ismerős képek és a szerver mappái

Az oldal feltehetőleg hibás beállítása miatt a teljes mappaszerkezet bejárható és hozzáférhető volt. A *crowcow.info* oldal láthatóan több, máshol hosztolt kampányt is kiszolgált, amelyek landing oldalai a *crowcow.info* oldal mappáiból töltötték be a képi elemeket.

A folderekben megtalálhatók és letölthetők voltak az aktorhoz tartozó kampányok tömörített mappaszerkezetei, valamint az egyes kampányok teljes fájlstruktúrája.

A kampányok egyezőségei miatt további kulcsszó, képi és fájlnév keresések segítségével olyan tartalmak voltak felfedhetők, amelyek más, a kampányok kiszolgálásában résztvevő szervereket vettek igénybe a landing oldalak szerkezeteinek tárolására.





localnewsreviews.com – landing mappaszerkezetek, side3.png

A kampányok vizsgálatakor korábban feltételezésre került, hogy valamilyen sablonrendszert használnak az álhírrel operáló landing oldalak tartalmainak megjelenítésére. A Csányi Sándor nevével visszaélő Bitcoin Loophole oldal részletesebb vizsgálatával ez a feltételezés igazolható.

Az oldal forrásának vizsgálatakor tapasztalható, hogy az oldal kódja nehezen olvasható és értelmezhető. Első ránézésre hiányoznak belőle a szöveges tartalmak, és a képi elemekre történő hivatkozások (például a side3.jpg), amelyekkel az oldal böngészésekor találkozhatunk.

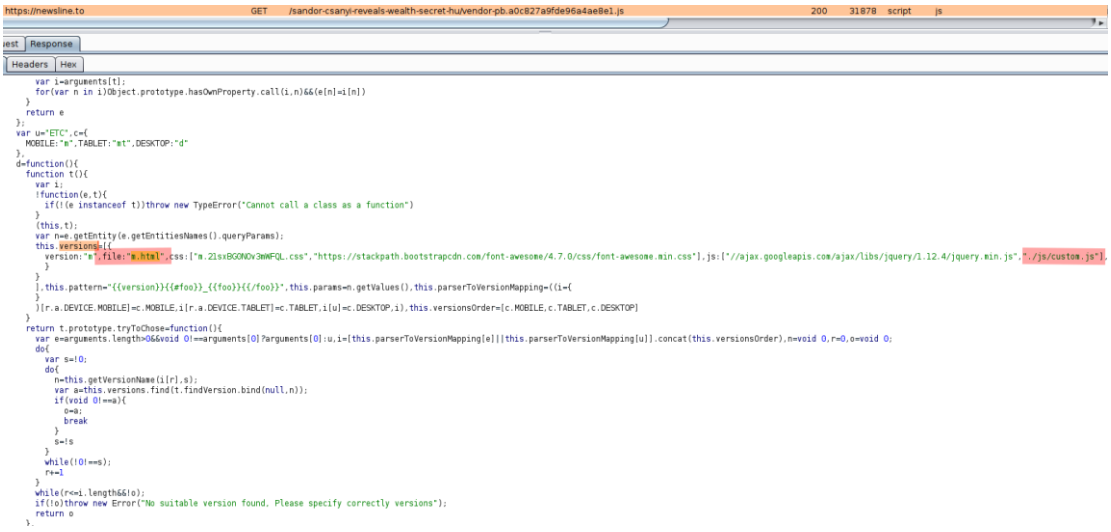
Az oldal kódja meglehetősen modern, nem hagyományos HTML szerkesztővel készítették, hanem a Webpack4 nevű, webes alkalmazások frontend felületinek fejlesztéséhez is használt eszközzel.

Az oldal Webpack4-alapú forrássa

Egy betöltött JavaScript kód

A *Burp* eszköz segítségével és webkiszolgálóval történő kommunikáció elemzésével a kód értelmezése és a JavaScript állományok „dekódolása” nélkül is hasznos információhoz lehetett jutni.

Megállapítható, hogy az oldal valóban sablonra épül, a Webpack4-alapú, JavaScript kódok töltik be, aktualizálják és jelenítik meg a sablon állományban található tartalmat.



A kommunikációból kinyert, a lefutó JavaScript kódok által generált tartalom

A forgalom vizsgálatával láthatóvá vált, hogy az oldal tényleges tartalma az „*m.html*" fájlban található, ezt a fájlt dolgozzák fel, majd jelenítik meg a különféle JavaScript állományok. Ha már ismert a szöveges és képi tartalmakat tároló sablon fájl neve, az már a böngészőből is behívható és megvizsgálható.

A fentebbi kép az először szélesebb nyilvánosságot kapó *https://newsline.to/sandor-csanyi-reveals-wealth-secret-hu* oldal vizsgálatakor készült, azonban ugyanez az állomány érhető el a *https://newsline.to/hu-sandor-csanyi-loophole* címen is.

m.html sablon

A sablonban három változó is megtalálható, például a *[dateNow]]*, *[[dateNow locales=hu]]* és *[[checkerCampid]]* változók, amelyeket az oldal betöltődésekor töltenek fel aktuális tartalommal a böngésző oldalon lefutó JavaScript kódok.

FRISSÍTÉS

Most kaptuk a híreket, hogy ma ([[dateNow locales=hu]]) óta szinte minden pozíció foglalt a magyar lakosok számára. A Bitcoin Loophole csak korlátozott számú felhasználót fogadhat el, hogy a felhasználónkénti profit magas értéken maradjon. Jelenleg még mindig van (37) szabad hely, **tehát siessen és iratkozzon fel most, hogy biztosan legyen helye!**.

FRISSÍTÉS

Most kaptuk a híreket, hogy ma (2020. szeptember 5., szombat) óta szinte minden pozíció foglalt a magyar lakosok számára. A Bitcoin Loophole csak korlátozott számú felhasználót fogadhat el, hogy a felhasználónkénti profit magas értéken maradjon. Jelenleg még mindig van (37) szabad hely, **tehát siessen és iratkozzon fel most, hogy biztosan legyen helye!**.

Az oldal betöltődésekor a dateNow változó mindig az aktuális napot jeleníti meg magyar formátumban

A nyilvános forrású információgyűjtés eszközeit és módszereit felhasználva egyértelműen megállapítható, hogy mind a nyelvi elemek, mind pedig az oldalak készítéséhez használt modern technológiák alapján a *https://newsline.to/sandor-csanyi-reveals-wealth-secret-hu* és a *https://newsline.to/hu-sandor-csanyi-loophole* oldalak ugyanannak a kampánynak a részei, tartalmukban, technológiájukban megegyeznek és feltehetőleg ugyanaz a személy helyezte el és működtette az oldalakat.

Terjedés, reklámok

A korábbi kampányok, például a Karácsony Gergely nevével visszaélő Bitcoin Era és Bitcoin Revolution esetében is tapasztalható volt, hogy az aktorok a tartalmakat a Google hirdetési felületein népszerűsítik. Bár csaló hirdetések lejelentésével ezek a reklámok viszonylag gyorsan lekapcsolhatók (a Google többnyire ilyenkor a hirdetői fiókot is letiltja), az ilyen hirdetések megjelenhetnek egyébként olyan megbízható oldalakon is, amelyek a Google AdSense szolgáltatását beépítik oldalaikba.

A Facebook 2019 óta küzd a különféle kriptovaluta-csalásokkal operáló hirdetésekkel, például 2019-ben nagy port kavart az Abu-Dhabi koronaherceg nevével visszaélő Bitcoin Loophole kampány, amely a Facebook hirdetési platformját használta a terjedésre[21]. A kampány meglehetősen sikeresnek volt mondható, rengeteg befektető adott meg személyes adatokat, illetve utalt pénzt a kampány mögött álló ukrán és argentin csalóknak.

Különös szerencse (?), hogy a Bitcoin Loophole OSINT vizsgálata közben a Facebook elkezdett Bitcoin Loophole hirdetéseket megjeleníteni, így a reklámokat és a mögöttes folyamatokat és tartalmakat is ellenőrizni lehetett.

[21] *https://cointelegraph.com/news/facebook-removes-bitcoin-scam-ads-with-abu-dhabi-crown-prince*

A „*MyTech*", az „*International Food*" és a „*We love mexican food*" oldalak által feladott hirdetések képi eleme egyértelműen ugyanarra a hálózatra utal. A képek bár kissé eltérnek egymástól, szövegezésüket tekintve megegyeznek. Mindhárom hirdetés úgy jelenik meg, mintha az Index.hu oldal híranyagát reklámoznák.

A hirdetéseket feladó oldalak ellenőrzésekor látható volt, hogy az oldalakat júliusban és augusztusban hozták létre. Mindhárom oldal esetében biztosan állítható, hogy kifejezetten csaló szándékkal létrehozott áloldalak, amelyek célja, hogy Facebook hirdetésekben népszerűsítsék a Bitcoin Loophole-t.

	Létrehozva	Követők	Domain/URL	Domain reg.	Landing
International Food	2017.07.17	1487	bestbasicnewz.com/hu	2020.07.14	newsline.to/hu-sandor-csanyi-loophole
MyTech	2020.06.06	957	besttechblogg.com/hu	2020.07.14	newsline.to/hu-sandor-csanyi-loophole
We love mexican food	2020.06.21	1822	superscienceway.com/hu	2020.07.14	newsline.to/hu-sandor-csanyi-loophole

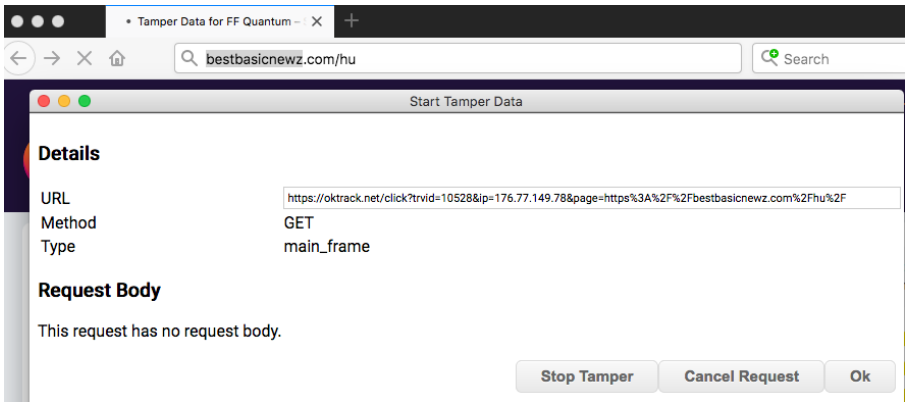
A reklámok linkjei különböző oldalra mutatnak, de a reklámokra linkelt oldalak csak továbbítóként és ajánlóként működnek, a látogatókat átirányítják a tényleges landing oldalra.

A linkekben szereplő domain címek utolsó regisztrációs dátuma 2020. július 14., ami feltételezi, hogy ugyanaz az aktor regisztrálta az oldalakat, azonban a *bestbasicnewz.com* esetében historikus keresésekkel megállapítható, hogy már korábban, 2020. március 13-án is beregisztrálták (vagy egyszer már lekapcsolták, esetleg havidíjas domain előfizetés volt és az előfizető nem finanszírozta tovább).

A reklámok alatt szereplő linkek lehetőséget adnak a továbbítási mechanizmus vizsgálatára.

Átirányítás és további tartalmak

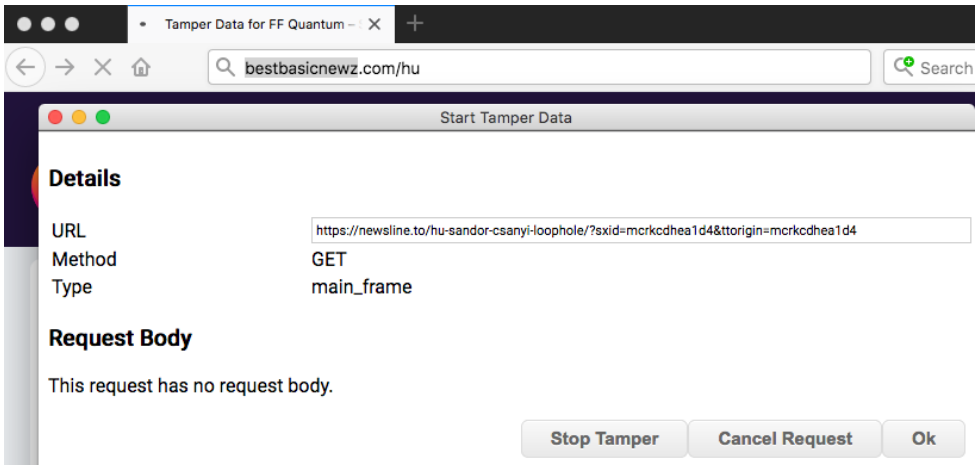
A *bestbasicnewz.com*, *besttechblogg.com* és *superscienceway.com* oldalak paraméterekkel látják el átirányításkor a címet.



A bestbasicnewz.com/hu átirányítja a látogatót az oktrack.net oldal felé

A paraméterekben szerepel egy feltehetőleg célállomás azonosító (*trvid*), azaz, hogy a következő átirányító szerver (*oktrack.net*) hova továbbítsa a látogatót, a látogató IP címe, valamint a forrás oldal, ahonnan az átirányítás történik (ajánló).

A *Tamper Data* böngészőkiegészítő segítségével ellenőrizhető, hogy a weboldal megjelenésekor milyen címekről honnan és milyen HTML objektumok töltődnek be, illetve hogy milyen átirányítások történnek a megjelenítés során.



Az oktrack.net tovább irányít a landing oldal felé

A második átirányító, az *oktrack.net* oldal az átirányításkor új paraméterekkel látja el a címet, majd továbbítja a látogatót a Csányi Sándor nevével visszaélő Bitcoin Loophole landing oldalra.

Reklám link	Átirányító	Landing
bestbasicnewz.com/hu	oktrack.net/click?trvid=10528	newsline.to/hu-sandor-csanyi-loophole
superscienceway.com/hu	oktrack.net/click?trvid=10541	newsline.to/hu-sandor-csanyi-loophole
besttechblogg.com/hu	oktrack.net/click?trvid=10624	newsline.to/hu-sandor-csanyi-loophole

A táblázatban összefoglalva látható, hogy a reklám oldalak az *oktrack.net* felé irányítják a látogatókat, illetve az is megállapítható, hogy mindegyik reklám oldal más *trvid* azonosítóval paraméterezi az átirányítást.

Ugyan a három reklám oldal esetében az átirányítás végállomása a *newsline.hu/hu-sandor-csanyi-loophole* oldal, az eltérő *trvid* azonosítók alapján feltételezhető, hogy az eltérő *trvid* azonosítók egyébként akár más-más végállomás felé is irányíthatnák a látogatót.

Mivel feltehetőleg az *oktrack.net* átirányítási pont biztosítja a kampányok vezérlését, azért a *trvid* paraméterben szereplő azonosítók is ellenőrzésre kerültek.

A *HeadmasterSEO* automata eszközzel a *trvid* értékeket 10001-től 10999-ig léptetve láthatóvá vált, hogy az *oktrack.net* szerver jelenleg 637 olyan átirányítást kezel, amely a Bitcoin Loophole kampány valamely landing oldalára vezet.

A landing oldalak lehetnek álhír tartalmak, mint például a Csányi Sándor nevével operáló oldal. Olyan esetekben, amikor nem készült álhír tartalom, az átirányító közvetlenül a Bitcoin Loophole kampány központi forgalomirányító oldalára (*trkpower.com*) vezeti a látogatót.

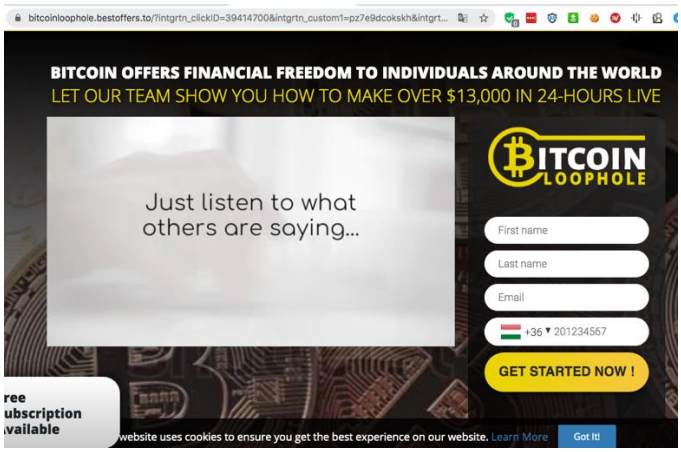
All URLs | Abort | Clear

URL	Type	Status Co...	Status	Size	Response Ti...	...	...	Redirect To Final URL
https://oktrack.net/click?trvid=10016	text/html;...	302	Found	131	0.85			https://trkpower.com/click.php?project_id=qd&affiliate_id=z9b&custom1=kjqyegew1jum&custom2...
https://oktrack.net/click?trvid=10017	text/html;...	302	Found	131	0.83			https://trkpower.com/click.php?project_id=qd&affiliate_id=z9b&custom1=szntxfz78750&custom2...
https://oktrack.net/click?trvid=10018	text/html;...	302	Found	131	0.80			https://trkpower.com/click.php?project_id=qd&affiliate_id=z9b&custom1=yyo5qpluc4rl&custom2=...
https://oktrack.net/click?trvid=10019	text/html;...	302	Found	131	0.79			https://trkpower.com/click.php?project_id=qd&affiliate_id=z9b&custom1=s967wq92ux4b&custom...
https://oktrack.net/click?trvid=10020	text/html;...	302	Found	131	0.77			https://trkpower.com/click.php?project_id=qd&affiliate_id=z9b&custom1=ivs6qc584jux&custom2...
https://oktrack.net/click?trvid=10021	text/html;...	302	Found	131	0.60			https://trkpower.com/click.php?project_id=qd&affiliate_id=z9b&custom1=nvvdy39z4zfa&custom2...
https://oktrack.net/click?trvid=10022	text/html;...	302	Found	131	0.57			https://trkpower.com/click.php?project_id=qd&affiliate_id=z9b&custom1=eb9v4ng8wk26&custom...
https://oktrack.net/click?trvid=10023	text/html;...	302	Found	131	0.56			https://trkpower.com/click.php?project_id=qd&affiliate_id=z9b&custom1=wjbvzyz6yook&custom2...
https://oktrack.net/click?trvid=10024	text/html;...	302	Found	131	0.53			https://trkpower.com/click.php?project_id=qd&affiliate_id=z9b&custom1=nevymbqbqiey&custom...
https://oktrack.net/click?trvid=10025	text/html;...	302	Found	131	0.42			https://trkpower.com/click.php?project_id=qd&affiliate_id=z9b&custom1=bvmfc98yxg6f&custom2...
https://oktrack.net/click?trvid=10026	text/html;...	302	Found	98	0.45			https://surfshark.com/deals?coupon=topvpnoffer&transaction_id={transaction_id}&offer_id={offer...
https://oktrack.net/click?trvid=10027	text/html;...	302	Found	98	0.44			https://surfshark.com/deals?coupon=topvpnoffer&transaction_id={transaction_id}&offer_id={offer...
https://oktrack.net/click?trvid=10028	text/html;...	302	Found	131	0.44			https://trkpower.com/click.php?project_id=qd&affiliate_id=z9b&custom1=i1m9u9nuviog&custom2...
https://oktrack.net/click?trvid=10029	text/html;...	302	Found	131	0.44			https://trkpower.com/click.php?project_id=qd&affiliate_id=z9b&custom1=804b4xlbi9ya&custom2...
https://oktrack.net/click?trvid=10030	text/html;...	302	Found	131	0.44			https://trkpower.com/click.php?project_id=qd&affiliate_id=8Db&custom1=k57prwoary3y&custom...
https://oktrack.net/click?trvid=10031	text/html;...	302	Found	107	1.39			https://247news.to/hu-meszaros-loophole/?sxid=r9qrjaugc4uc&ttorigin=r9qrjaugc4uc
https://oktrack.net/click?trvid=10032	text/html;...	302	Found	131	0.43			https://trkpower.com/click.php?project_id=qd&affiliate_id=8Db&custom1=co9asmitqac9&custom...
https://oktrack.net/click?trvid=10033	text/html;...	302	Found	131	0.44			https://trkpower.com/click.php?project_id=qd&affiliate_id=8Db&custom1=slz3b3q725ie&custom2...
https://oktrack.net/click?trvid=10034	text/html;...	302	Found	131	0.44			https://trkpower.com/click.php?project_id=qd&affiliate_id=8Db&custom1=g85p3q8ewotj&custom...
https://oktrack.net/click?trvid=10035	text/html;...	302	Found	131	0.44			https://trkpower.com/click.php?project_id=qd&affiliate_id=8Db&custom1=o7k6j9buwfmq&custom...
https://oktrack.net/click?trvid=10036	text/html;...	302	Found	131	0.44			https://trkpower.com/click.php?project_id=qd&affiliate_id=8Db&custom1=79e35wkfnxwo&custom...

HTTP kérések és a böngészés automatizálása

A HeadmasterSEO automata eszköz végig látogatta az *oktrack.net/click?trvid=10001* és *oktrack.net/click?trvid=10999* közötti címeket, és rögzítette, hogy az egyes átirányítások hova továbbítanák a látogatókat.

A vizsgált 1000 *trvid* paraméterből 637 működő átirányítás található. Ebből 44 mutat a Bitcoin Loophole valamely álhírrel operáló landing oldalára, míg a *trkpower.com*-ra mutató átirányítások a *bitcoinloophole.bestoffers.com* oldalra vezetnek, amely láthatóan a Bitcoin Loophole scam egyik adatbegyűjtő regisztrációs oldala.



bitcoinloophole.bestoffers.com – az adatgyűjtő és regisztrációs oldal

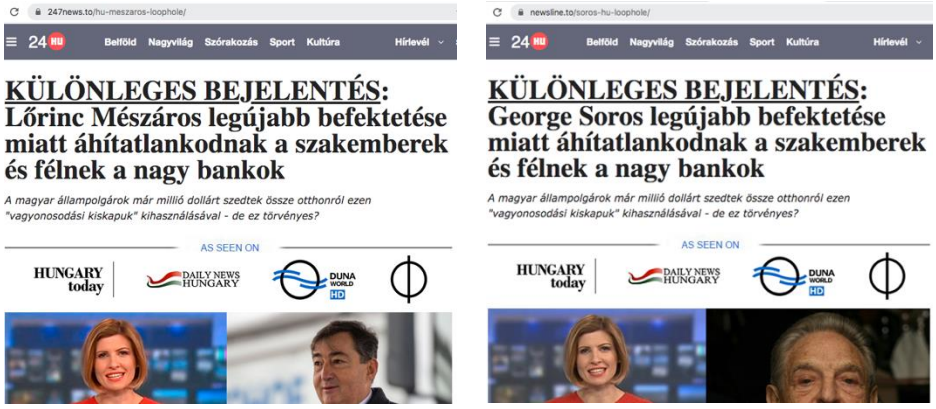
Feltételezhető, hogy a *trkpower.com*-os átirányítások olyan kampányvezérlők, amelyek még nem kerültek felhasználásra, vagy pedig olyan kampányvezérlők, amelyekhez nem tartottak szükségesnek álhír tartalmat készíteni.

A 44 olyan átirányítást vizsgálva, amely a kampányhoz tartozó álhíroldalakra vezeti a látogatót, megállapítható, hogy nem csak Csányi Sándor nevével, de Mészáros Lőrinc és Soros György nevével is reklámozzák a „szolgáltatást”.

Átirányítás, azonosító	Scam landing oldal
oktrack.net/click?trvid=10031	247news.to/hu-meszaros-loophole
oktrack.net/click?trvid=10060	247news.to/hu-meszaros-loophole
oktrack.net/click?trvid=10096	247news.to/hu-meszaros-loophole
oktrack.net/click?trvid=10109	247news.to/hu-meszaros-loophole
oktrack.net/click?trvid=10112	247news.to/hu-meszaros-loophole

oktrack.net/click?trvid=10139	247news.to/hu-meszaros-loophole
oktrack.net/click?trvid=10162	newsline.to/hu-sandor-csanyi-loophole
oktrack.net/click?trvid=10168	newsline.to/hu-sandor-csanyi-loophole
oktrack.net/click?trvid=10500	247news.to/hu-meszaros-loophole
oktrack.net/click?trvid=10515	newsline.to/hu-sandor-csanyi-loophole
oktrack.net/click?trvid=10527	newsline.to/soros-hu-loophole
oktrack.net/click?trvid=10528	newsline.to/hu-sandor-csanyi-loophole
oktrack.net/click?trvid=10541	newsline.to/hu-sandor-csanyi-loophole
oktrack.net/click?trvid=10565	247news.to/hu-meszaros-loophole
oktrack.net/click?trvid=10566	247news.to/hu-meszaros-loophole
oktrack.net/click?trvid=10584	newsline.to/hu-sandor-csanyi-loophole
oktrack.net/click?trvid=10598	247news.to/hu-meszaros-loophole
oktrack.net/click?trvid=10603	newsline.to/hu-sandor-csanyi-loophole
oktrack.net/click?trvid=10604	newsline.to/hu-sandor-csanyi-loophole
oktrack.net/click?trvid=10605	newsline.to/hu-sandor-csanyi-loophole
oktrack.net/click?trvid=10608	newsline.to/hu-sandor-csanyi-loophole
oktrack.net/click?trvid=10617	newsline.to/hu-sandor-csanyi-loophole
oktrack.net/click?trvid=10619	newsline.to/hu-sandor-csanyi-loophole
oktrack.net/click?trvid=10621	247news.to/hu-meszaros-loophole
oktrack.net/click?trvid=10624	newsline.to/hu-sandor-csanyi-loophole
oktrack.net/click?trvid=10632	newsline.to/hu-sandor-csanyi-loophole

Az összefoglaló táblázatból látható, hogy mely *oktrack.net* átirányítások milyen hazai érintettségű, álhír tartalmú landing oldalra vezetnek. Az új elemeket ellenőrizve megállapítható, hogy a Mészáros Lőrinc és Soros György nevével visszaélő tartalmak teljesen megegyeznek a Csányi Sándor nevével visszaélő tartalommal.



Újabb tartalmak, Mészáros Lőrinc és Csányi Sándor

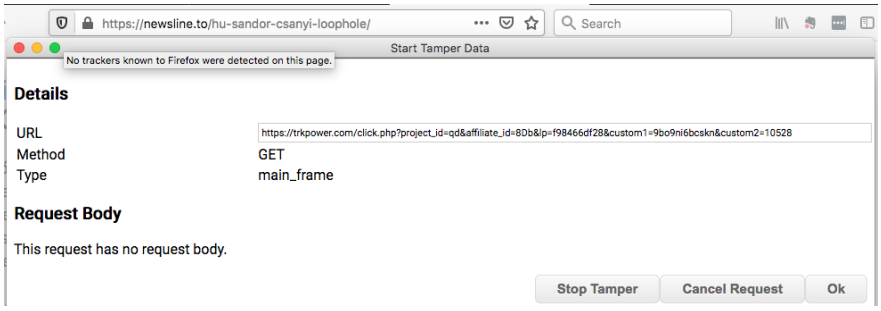
A már ismert *newsline.to* cím mellett láthatóvá vált egy *247news.to* cím is, amelyen a Mészáros Lőrinc nevével operáló landing oldal található. Erről az oldalról eddig csak a *profitline.hu*[22] számolt be 2020. augusztus 31-én[23].

[22] *http://profitline.hu/Meszaros-Lorinc-et-felhasznalva-terjed-egy-hamisitott-24.hu-a-Facebookon-411609*

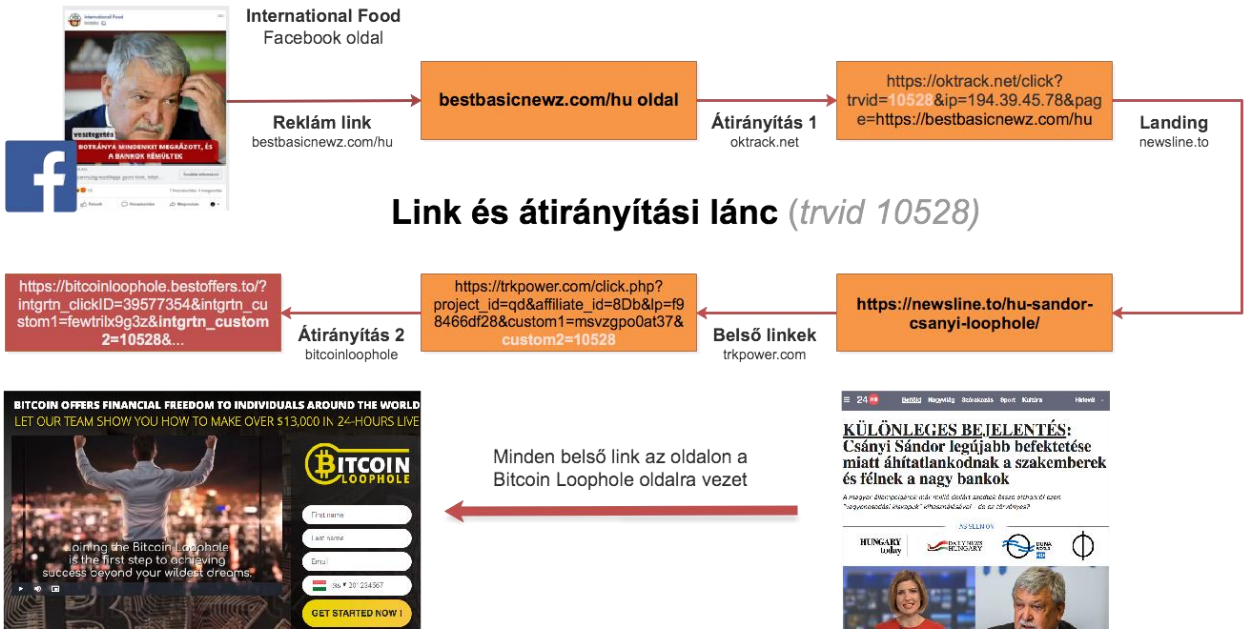
[23] *Jelen tanulmány írásának megkezdésekor (2020. augusztus 12.) ez a tartalom még nem volt ismert.*

Az álhír tartalmú oldalak belső linkjeire kattintva egy újabb átirányításon keresztül (*trkpower.com*) arra a *bitcoinloophole.bestoffers.to* címre jut a látogató, amelyet már láthattunk az átirányítások tesztelésekor.

A továbbítások itt is paraméterezésre kerülnek. A paraméterek tartalmazzák a korábbi *trvid* értéket, valamint affiliate azonosítót (*affiliate_id*) rendelnek a címekhez. Ebből feltételezhető, hogy a *bitcoinloophole.bestoffers.to* az adatgyűjtés és természetesen a látogatók pénzének kicsalása mellett elszámoló központként is működik, amely a kampányban résztvevő aktorok jutalékait számolja el.



A newsline.to oldalak bármely belső címére kattintva egy újabb átirányítás történik



A Facebook reklámokkal támogatott kampányok működése

Összefoglalás

A fentebb ismertetett Bitcoin Loophole, illetve a bemutatott kampány csak egy, a különféle kriptovalutás csalás közül. Akár sokszáz vagy többezer hasonló, a kriptovaluták népszerűségét kihasználó csalás létezik, amelyek felderítéséhez rengeteg erőforrásra lenne szükség.

A *bitcoinloophole.bestoffers.to* központi oldal vizsgálatával jelen tanulmány nem foglalkozik, mivel az oldal ellenőrzésekor olyan információk kerültek feltárásra, amelyek alapján az oldal vizsgálata egy későbbi tanulmányban kerül dokumentálásra.

A csalók láthatóan fejlett, jól működő rendszereket használnak, amelyek összehangoltan és automatizáltan működnek.

A sablonrendszer és az affiliate azonosítók használata feltételezi, hogy egy partnerprogram-jellegű hálózat áll a Bitcoin Loophole (és a hasonló kampányok) mögött, ahol a „partnerprogram" résztvevői a működtető infrastruktúráját (sablonok, templatek, átirányítók és központi oldal) használják. A partnereknek csak az álhírtartalmak gyártása (amelyhez a sablonrendszer rendelkezésre áll), illetve a reklámok kihelyezése a feladatuk, amelyért cserébe részesülnek a *bitcoinloophole.bestoffers.to* oldalra vezetett látogatóktól kicsalt összegekből.

A *bitcoinloophole.bestoffers.to* oldalon begyűjtött személyes adatokkal kapcsolatban feltételezhető, hogy azok további csalások során kerülhetnek felhasználásra. Az ilyen jellegű információk meglehetősen értékesnek számítanak, főleg olyan esetben, ahol láthatóan egy fogékony áldozat adatairól van szó. Ha egyszer becsapható volt az óvatlan és hiányos biztonságtudatosságú áldozat, akkor a későbbiekben is jó lehetőségeket láthatnak a csalásra szakosodott bűnözők. A becsapottak valószínűleg nem fognak többé kriptovalutába vagy kereskedési platformokba fektetni, azonban más csalásra sajnos nyitottak lehetnek.

Felmerül a kérdés, hogyan lehet védekezni az álhírekkel ötvözött és csalási szándékkal létrehozott oldalakkal szemben?

Jelenleg nem létezik olyan technológia, amely képes lenne az ilyen tartalmakat kiszűrni. Ha csak az álhíreket vizsgáljuk, megjelentek már a mesterséges intelligencia felhasználására tett törekvések, azonban az ilyen megoldások gyermekcipőben járnak, a közeljövőben még nem fognak biztos megoldást jelenteni.

A hír- és tényellenőrző szolgáltatások (*fact checker*) jelenleg az emberi erőforrásokra támaszkodnak, de korántsem tökéletesek. Nehezen zárják ki azokat az emberi tényezőket, amelyekkel a mesterséges intelligenciáknak nem kell megküzdenie (például a tényszerűséget erodáló érzelmeket és szubjektivitást).

A legműködőképesebb megoldásnak a felhasználók (internet használók) biztonságtudatosságának fejlesztése látszik. Az értő olvasás mellett a felhasználónak tisztában kell lennie a rá leselkedő veszélyekkel, és át kell látnia a „fantasztikusan jó ajánlatok" manipulatív kommunikációján.

A Bitcoin Loophole és a hasonló, hihetetlen hozamokat kínáló befektetések ígérete gyanút kell, hogy ébresszen és a felhasználónak fel kell tennie magának a kérdést: *Nem túl szép ez ahhoz, hogy igaz legyen?* Ha a kétely ráveszi a felhasználót, hogy utána nézzen a „kihagyhatatlan ajánlatnak" (például egyszerű rákereséssel vagy akár OSINT módszerek alkalmazásával), sokkal nehezebb dolga lesz a csalóknak és sokkal kevesebb áldozata lesz a tevékenységüknek.

Jelen tanulmány célja kettős volt. Szerettük volna bemutatni a Bitcoin Loophole kampány működését és jellegzetességeit, valamint olyan dokumentumot szerettünk volna összeállítani, amely bemutatja a nyilvános forrású információgyűjtés (OSINT) lehetőségeit, eszközeit az ilyen vizsgálatok során.

Ahogy a bevezetőben is említésre került, a nyilvános forrású információgyűjtés nem kötődik szakmához vagy hivatáshoz: a nyilvános forrásokban történő keresés, kutatás és információgyűjtés bárki számára elérhető, megkönnyítheti feladata teljesítését és céljai elérését. Jelen esetben ez a cél a Bitcoin Loophole kripto-fraud hálózat felderítése volt, amelyet az OSINT módszerek és eszközök használatával értünk el.